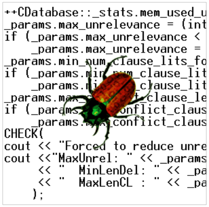
# Bounded Model Checking with SAT/SMT

Edmund M. Clarke

School of Computer Science
Carnegie Mellon University



```
++CDatabase::_stats.mem_used_u
_params.max_unrelevance = (int
if (_params.max_unrelevance <
    _params.max_unrelevance =
_params.min_num_clause_lits_fo
if (_params.min   m_clause_lit
    _params.         clause_lit
_params.ma          t_clause_le
if (_params.         onflict_claus
    _params.ma  conflict_claus
CHECK(
cout << "Forced to reduce unre
cout <<"MaxUnrel: " << _params
     << "  MinLenDel: " << _pa
     << "  MaxLenCL : " << _pa
    );
```

## Recap: Symbolic Model Checking with BDDs

Method used by most "industrial strength" model checkers:

- uses Boolean encoding for state machine and sets of states.
- can handle much larger designs – hundreds of state variables.
- BDDs traditionally used to represent Boolean functions.

## Problems with BDDs

- BDDs are a canonical representation. Often become too large.
- Variable ordering must be uniform along paths.
- Selecting right variable ordering very important for obtaining small BDDs.
  - Often time consuming or needs manual intervention.
  - Sometimes, no space efficient variable ordering exists.

**Bounded Model Checking (BMC) is an alternative approach to symbolic model checking that uses SAT procedures.**

## Advantages of SAT Procedures

- SAT procedures also operate on Boolean expressions but do not use canonical forms.
- Do not suffer from the potential space explosion of BDDs.
- Different split orderings possible on different branches.
- Very efficient implementations available.

## Bounded Model Checking (Clarke, Biere, Cimatti, Zhu)

- Bounded model checking uses a SAT procedure instead of BDDs.
- We construct Boolean formula that is satisfiable iff there is a counterexample of length $k$.
- We look for longer and longer counterexamples by incrementing the bound $k$.

## Bounded Model Checking (Cont.)

- After some number of iterations, we may conclude no counterexample exists and specification holds.
- For example, to verify safety properties, number of iterations is bounded by diameter of finite state machine.

## Main Advantages of Our Approach

- Bounded model checking finds counterexamples fast. This is due to depth first nature of SAT search procedures.
- It finds counterexamples of minimal length. This feature helps user understand counterexample more easily.

## Main Advantages of Our Approach (Cont.)

- It uses much less space than BDD based approaches.
- Does not need manually selected variable order or costly reordering. Default splitting heuristics usually sufficient.
- Bounded model checking of LTL formulas does not require a tableau or automaton construction.

## Implementation

- Implemented a tool BMC in 1999.
- It accepts a subset of the SMV language.
- Given $k$, BMC outputs a formula that is satisfiable iff counterexample exists of length $k$.
- If counterexample exists, a standard SAT solver generates a truth assignment for the formula.

## Performance

- There are many examples where BMC significantly outperforms BDD based model checking.
- In some cases BMC detects errors instantly, while SMV fails to construct BDD for initial state.
- Armin's example: Circuit with 9510 latches, 9499 inputs. BMC formula has $4 \times 10^6$ variables, $1.2 \times 10^7$ clauses. Shortest bug of length 37 found in 69 seconds.

## Temporal Logic

- We use linear temporal logic (LTL) for specifications.
- Basic LTL operators:

| | | | |
|---|---|---|---|
| *next time* | '$\mathbf{X}$' | *eventuality* | '$\mathbf{F}$' |
| *globally* | '$\mathbf{G}$' | *until* | '$\mathbf{U}$' |
| *release* | '$\mathbf{R}$' | | |

## Temporal Logic

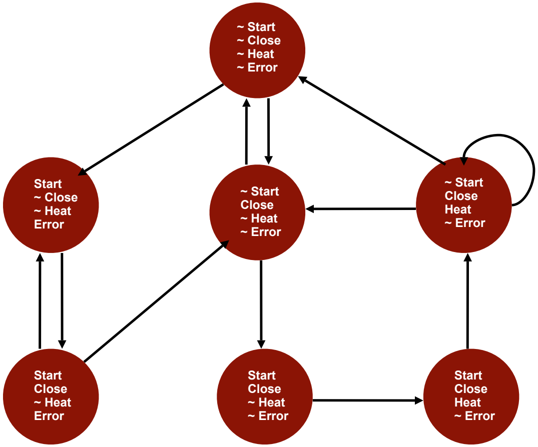
- Only consider existential LTL formulas $\mathbf{E}f$, where
  - $\mathbf{E}$ is the existential path quantifier, and
  - $f$ is a temporal formula with no path quantifiers.
- Finding a witness for $\mathbf{E}f$ is equivalent to finding a counterexample for $\mathbf{A}\neg f$.

## Kripke Structure

- System described as a Kripke structure $M = (S, I, T, \ell)$, where
  - $S$ is a finite set of states and $I$ a set of initial states,
  - $T \subseteq S \times S$ is the transition relation,
    (We assume every state has a successor state.)
  - $\ell \colon S \to \mathcal{P}(\mathcal{A})$ is the state labeling.

## The Microwave Oven Example

$$\mathbf{AG}(\mathit{start} \rightarrow (\neg \mathit{heat}\ \mathbf{U}\ \mathit{close}))$$



~ Start ~ Close ~ Heat ~ Error
Start ~ Close ~ Heat Error
~ Start Close ~ Heat ~ Error
~ Start Close Heat ~ Error
Start Close ~ Heat Error
Start Close ~ Heat ~ Error
Start Close Heat ~ Error

## Diameter

- Diameter $d$: Least number of steps to reach all reachable states. If the property holds for $k \geq d$, the property holds for all reachable states.
- Finding $d$ is computationally hard:
  - State $s$ is reachable in $j$ steps:

$$R_j(s) := \exists s_0, \ldots, s_j : s = s_j \wedge I(s_0) \wedge \bigwedge_{i=0}^{j-1} T(s_i, s_{i+1})$$

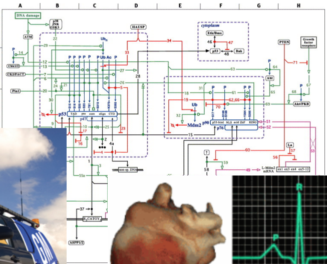
  - Thus, $k$ is greater or equal than the diameter $d$ if

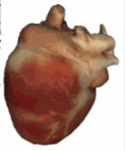
$$\forall s : R_{k+1}(s) \Longrightarrow \exists j \leq k : R_j(s)$$

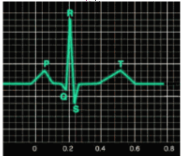
**This requires an efficient QBF checker!**

## The Cyber-Physical Challenge

- Complex aerospace, automotive, biological systems.
- They combine discrete and continuous behaviors.
- Many are safety-critical.







## Bounded Model Checking for Hybrid Automata

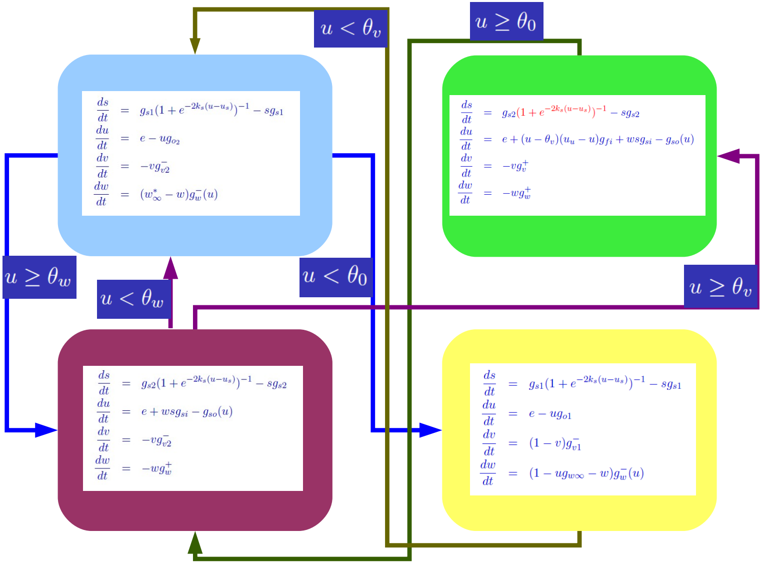
- Hybrid automata [Alur et al. 1992] are widely used to model cyber-physical systems.
- They combine finite automata with continuous dynamical systems.
- Grand challenge for formal verification!
  - Reachability for simple systems is undecidable.
  - Existing tools do not scale on realistic systems.

## Hybrid Systems

$\mathcal{H} = \langle X, Q, \mathsf{Init}, \mathsf{Flow}, \mathsf{Jump} \rangle$

- A continuous space $X \subseteq \mathbb{R}^k$ and a finite set of modes $Q$.
- Init $\subseteq Q \times X$: initial configurations
- Flow: continuous flows
  - Each mode $q$ is equipped with differential equations $\dfrac{d\vec{x}}{dt} = \vec{f}_q(\vec{x}, t)$.
- Jump: discrete jumps
  - The system can be switched from $(q, \vec{x})$ to $(q', \vec{x}')$, resetting modes and variables.

# Example: Cardiac-Cell Model



$$\begin{aligned}\frac{ds}{dt} &= g_{s1}(1+e^{-2k_s(u-u_s)})^{-1} - sg_{s1}\\ \frac{du}{dt} &= e - ug_{o_2}\\ \frac{dv}{dt} &= -vg_{v2}^{-}\\ \frac{dw}{dt} &= (w_\infty^{*} - w)g_w^{-}(u)\end{aligned}$$

$$\begin{aligned}\frac{ds}{dt} &= g_{s2}(1+e^{-2k_s(u-u_s)})^{-1} - sg_{s2}\\ \frac{du}{dt} &= e + (u-\theta_v)(u_u - u)g_{fi} + wsg_{si} - g_{so}(u)\\ \frac{dv}{dt} &= -vg_v^{+}\\ \frac{dw}{dt} &= -wg_w^{+}\end{aligned}$$

$$\begin{aligned}\frac{ds}{dt} &= g_{s2}(1+e^{-2k_s(u-u_s)})^{-1} - sg_{s2}\\ \frac{du}{dt} &= e + wsg_{si} - g_{so}(u)\\ \frac{dv}{dt} &= -vg_{v2}^{-}\\ \frac{dw}{dt} &= -wg_w^{+}\end{aligned}$$

$$\begin{aligned}\frac{ds}{dt} &= g_{s1}(1+e^{-2k_s(u-u_s)})^{-1} - sg_{s1}\\ \frac{du}{dt} &= e - ug_{o1}\\ \frac{dv}{dt} &= (1-v)g_{v1}^{-}\\ \frac{dw}{dt} &= (1 - ug_{w\infty} - w)g_w^{-}(u)\end{aligned}$$

# Reachability for Continuous Systems

Single differential equation case:

- Continuous Dynamics: $\frac{d\vec{x}(t)}{dt} = \vec{f}(\vec{x}(t), t)$
  - The solution curve:
    $\alpha : \mathbb{R} \to X,\ \alpha(t) = \alpha(0) + \int_0^t \vec{f}(\alpha(s), s)ds.$
  - Define the predicate
    $[\![\mathsf{Flow}(\vec{x}_0, t, \vec{x})]\!]^{\mathcal{M}} = \{(\vec{x}_0, t, \vec{x}) : \alpha(0) = \vec{x}_0, \alpha(t) = \vec{x}\}$
- Reachability: Is it possible to reach an unsafe state from an initial state following trajectory of differential equations?
  - $\exists \vec{x}_0, \vec{x}, t.\ (\mathsf{Init}(\vec{x}_0) \wedge \mathsf{Flow}(\vec{x}_0, t, \vec{x}) \wedge \mathsf{Unsafe}(\vec{x}))$ ?

## Reachability for Hybrid Systems

Combining continuous and discrete behaviors, we can encode bounded reachability:

- "$\vec{x}$ is reachable after after $0$ discrete jumps":

$$\mathsf{Reach}^0(\vec{x}) := \quad \exists \vec{x}_0, t.\ [\mathsf{Init}(\vec{x}_0) \wedge \mathsf{Flow}(\vec{x}_0, t, \vec{x})]$$

- Inductively, "$\vec{x}$ is reachable after $k+1$ discrete jumps" is definable as:

$$\mathsf{Reach}^{k+1}(\vec{x}) := \exists \vec{x}_k, \vec{x}'_k, t.\ [\mathsf{Reach}^k(\vec{x}_k) \wedge \mathsf{Jump}(\vec{x}_k, \vec{x}'_k) \wedge \mathsf{Flow}(\vec{x}'_k, t, \vec{x})]$$

- Unsafe within $n$ discrete jumps:

$$\exists \vec{x}.\ (\bigvee_{i=0}^{n} \mathsf{Reach}^i(\vec{x}) \wedge \mathsf{Unsafe}(\vec{x}))\ ?$$

## A Major Obstacle

We have shown how to use first-order formulas over the real numbers to encode formal verification problems for hybrid automata.

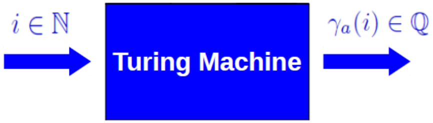
- Need to decide the truth value of formulas, which include nonlinear real functions.
  - Polynomials
  - Exponentiation and trigonometric functions
  - Solutions of ODEs, mostly no closed forms
- High complexity for polynomials; undecidable for either $\sin$ or $\cos$.

## Connection to Type 2 Computability

- Negative results put a limit on symbolic decision procedures for the theory over nonlinear real functions.
- In practice (control engineering, scientific computing) these functions are routinely computed numerically.
- Can we use numerical algorithms to decide logic formulas over the reals?

## Computable Real Numbers

- A real number $a \in \mathbb{R}$ is computable if it has a name $\gamma_a : \mathbb{N} \to \mathbb{Q}$ that is a total computable function.
    - $0.33\ldots$, $\sqrt{2}$, $\pi$, $e$, $0.101010010001000001\ldots$



- Not all reals are computable!
    - There are only countably many Turing machines while there are uncountably many real numbers.

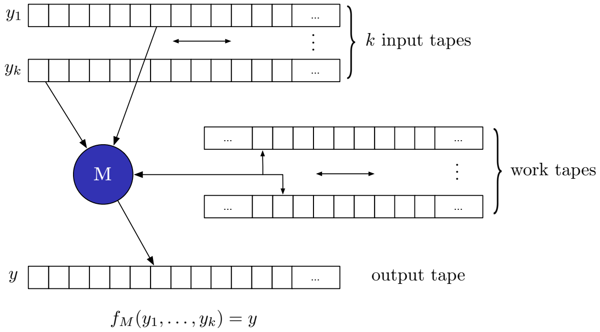
## Quote from Turing's 1936 Paper

- "Equally easy to define and investigate computable functions of an integral variable or a real or computable variable."
  - A. M. Turing, On Computable Numbers with an Application to the Entscheidungsproblem, Proceedings of the London Math Society, 1936.
- A real function $f$ is computable, if there exists a Type 2 Turing Machine that maps any name $\gamma_a$ of $a$ to a name $\gamma_{f(a)}$ of $f(a)$.

## Type 2 Turing Machines

A Type 2 Turing Machine extends an ordinary (Type 1) Turing Machine in the following way.

- Both the input tapes are infinite and read-only.
- The output tape is infinite and one-way.



## Connection to Type 2 Computability

- Type 2 computability gives a theoretical model of numerical computation.
  - $\exp$, $\sin$, ODEs are all Type 2 computable functions.
- We have developed a special type of decision procedure for first-order theories over the reals with Type 2 computable functions.
  - [Gao, Avigad, Clarke LICS2012, IJCAR2012].

## Perturbations on Logic Formulas

Satisfiability of quantifier-free formulas under numerical perturbations:

- Consider any formula

$$\varphi : \ \bigwedge_i (\bigvee_j f_{ij}(\vec{x}) = 0)$$

  - Inequalities are turned into interval bounds on slack variables.

- For any $\delta \in \mathbb{Q}^+$, let $\vec{c}$ be a constant vector satisfying $||\vec{c}||_{\max} \leq \delta$. A $\delta$-perturbation on $\varphi$ is the formula:

$$\varphi^{\vec{c}} : \ \bigwedge_i (\bigvee_j f_{ij}(\vec{x}) = c_{ij})$$

## The $\delta$-Decision Problem

We developed a decision procedure using numerical techniques (with an error bound $\delta$) that guarantees:

- If $\varphi$ is decided as "unsatisfiable", then it is indeed unsatisfiable.
- If $\varphi$ is decided as "$\delta$-satisfiable", then:

Under some $\delta$-perturbation $\vec{c}$, $\varphi^{\vec{c}}$ is satisfiable.

If a decision procedure satisfies this property, we say it is "$\delta$-complete".

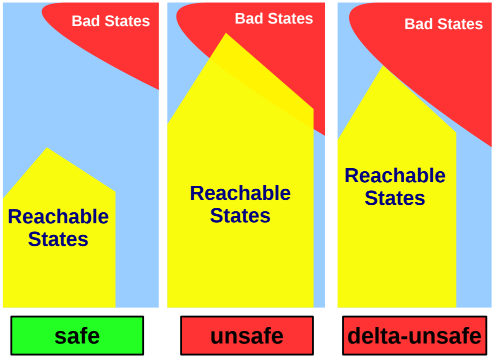
## Decidability and Complexity

- The delta-decision problem is decidable for bounded first-order formulas over arbitrary Type 2 computable functions.
- Complexity: (using [Ko 1991, Weihrauch 2000, Kawamura 2010])
  - $\mathbf{NP}$-complete for existential formulas in $\{+, \times, \exp, \sin, ...\}$.
  - $\mathbf{PSPACE}$-complete for existential formulas with ODEs.
- Note the difference: The strict decision problems are all undecidable for these signatures.
- This is not bad news: Modern SAT/SMT solvers can often handle many $\mathbf{NP}$-complete problems in practice.

# Delta-Complete Bounded Model Checking

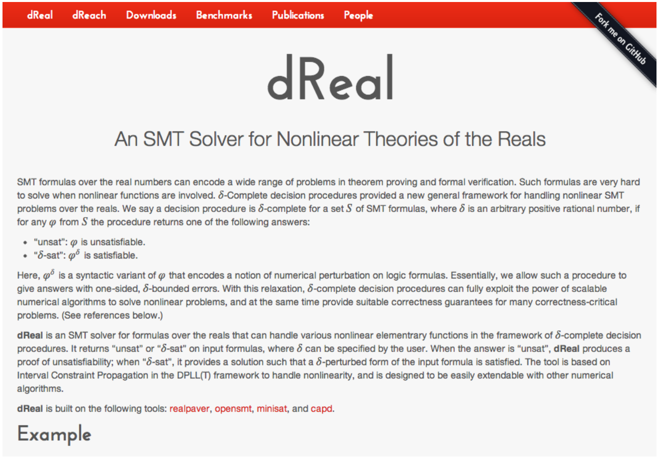
Recall that when bounded model checking a hybrid system $\mathcal{H}$, we ask if $\varphi : \text{Reach}_{\mathcal{H}}^{\leq n}(\vec{x}) \wedge \text{Unsafe}(\vec{x})$ is satisfiable.

- If $\varphi$ is **unsatisfiable**, then $\mathcal{H}$ is safe up to depth $n$.
- If $\varphi$ is $\delta$-**satisfiable**, then $\mathcal{H}$ is unsafe under some $\delta$-perturbation.



## Practical tool: dReal

Our solver dReal is open-source at dreal.cs.cmu.edu.



# dReal

## An SMT Solver for Nonlinear Theories of the Reals

SMT formulas over the real numbers can encode a wide range of problems in theorem proving and formal verification. Such formulas are very hard to solve when nonlinear functions are involved. $\delta$-Complete decision procedures provided a new general framework for handling nonlinear SMT problems over the reals. We say a decision procedure is $\delta$-complete for a set $S$ of SMT formulas, where $\delta$ is an arbitrary positive rational number, if for any $\varphi$ from $S$ the procedure returns one of the following answers:

- "unsat": $\varphi$ is unsatisfiable.
- "$\delta$-sat": $\varphi^\delta$ is satisfiable.

Here, $\varphi^\delta$ is a syntactic variant of $\varphi$ that encodes a notion of numerical perturbation on logic formulas. Essentially, we allow such a procedure to give answers with one-sided, $\delta$-bounded errors. With this relaxation, $\delta$-complete decision procedures can fully exploit the power of scalable numerical algorithms to solve nonlinear problems, and at the same time provide suitable correctness guarantees for many correctness-critical problems. (See references below.)

**dReal** is an SMT solver for formulas over the reals that can handle various nonlinear elementrary functions in the framework of $\delta$-complete decision procedures. It returns "unsat" or "$\delta$-sat" on input formulas, where $\delta$ can be specified by the user. When the answer is "unsat", **dReal** produces a proof of unsatisfiability; when "$\delta$-sat", it provides a solution such that a $\delta$-perturbed form of the input formula is satisfied. The tool is based on Interval Constraint Propagation in the DPLL(T) framework to handle nonlinearity, and is designed to be easily extendable with other numerical algorithms.

**dReal** is built on the following tools: realpaver, opensmt, minisat, and capd.

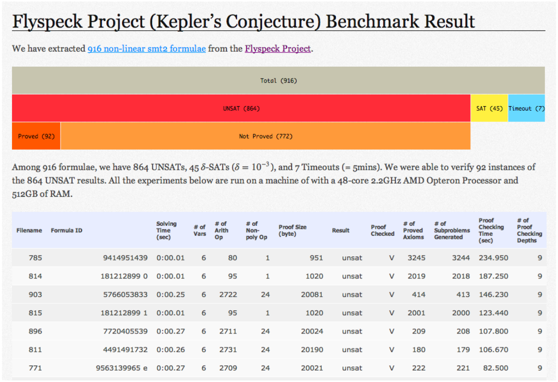
### Example

## dReal

- Nonlinear signatures including exp, sin, etc., and Lipschitz-continuous ODEs.
- dReal is $\delta$-complete.
- Proofs of correctness are provided.
- Tight integration of DPLL(T), interval arithmetic, constraint solving, reliable integration, etc.

# Example: Kepler Conjecture Benchmarks

- Around 1000 formulas. Huge combinations of nonlinear terms.
- dReal solves over 95% of the formulas. (5-min timeout each)



## Flyspeck Project (Kepler's Conjecture) Benchmark Result

We have extracted 916 non-linear smt2 formulae from the Flyspeck Project.

Total (916)

UNSAT (864) SAT (45) Timeout (7)

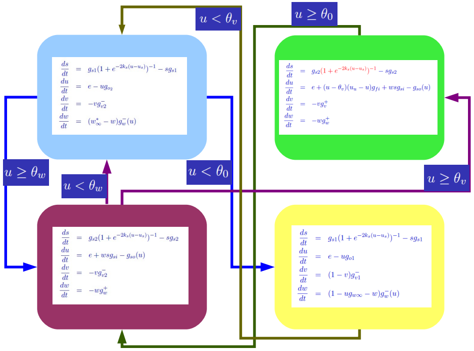
Proved (92) Not Proved (772)

Among 916 formulae, we have 864 UNSATs, 45 $\delta$-SATs ($\delta = 10^{-3}$), and 7 Timeouts (= 5mins). We were able to verify 92 instances of the 864 UNSAT results. All the experiments below are run on a machine of with a 48-core 2.2GHz AMD Opteron Processor and 512GB of RAM.

| Filename | Formula ID | Solving Time (sec) | # of Vars | # of Arith Op | # of Non-poly Op | Proof Size (byte) | Result | Proof Checked | # of Proved Axioms | # of Subproblems Generated | Proof Checking Time (sec) | # of Proof Checking Depths |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 785 | 9414951439 | 0:00.01 | 6 | 80 | 1 | 951 | unsat | V | 3245 | 3244 | 234.950 | 9 |
| 814 | 181212899 0 | 0:00.01 | 6 | 95 | 1 | 1020 | unsat | V | 2019 | 2018 | 187.250 | 9 |
| 903 | 5766053833 | 0:00.25 | 6 | 2722 | 24 | 20081 | unsat | V | 414 | 413 | 146.230 | 9 |
| 815 | 181212899 1 | 0:00.01 | 6 | 95 | 1 | 1020 | unsat | V | 2001 | 2000 | 123.440 | 9 |
| 896 | 7720405539 | 0:00.27 | 6 | 2711 | 24 | 20024 | unsat | V | 209 | 208 | 107.800 | 9 |
| 811 | 4491491732 | 0:00.26 | 6 | 2731 | 24 | 20190 | unsat | V | 180 | 179 | 106.670 | 9 |
| 771 | 9563139965 e | 0:00.27 | 6 | 2709 | 24 | 20021 | unsat | V | 222 | 221 | 82.500 | 9 |

## Example: Cardiac-Cell Model

- The cardiac-cell model is a hybrid system that contains nonlinear differential equations.
  - No existing formal analysis tool can analyze this model.
- The unsafe states of the model lead to serious cardiac disorder.

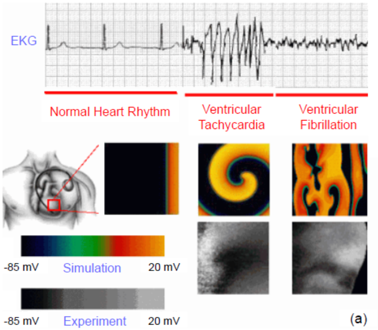


$\frac{ds}{dt} = g_{s1}(1+e^{-2k_s(u-u_s)})^{-1} - sg_{s1}$
$\frac{du}{dt} = e - ug_{o_2}$
$\frac{dv}{dt} = -vg_{v2}^{-}$
$\frac{dw}{dt} = (w_\infty^* - w)g_w^{-}(u)$
$\frac{ds}{dt} = g_{s2}(1+e^{-2k_s(u-u_s)})^{-1} - sg_{s2}$
$\frac{du}{dt} = e + (u-\theta_v)(u_u - u)g_{fi} + wsg_{si} - g_{so}(u)$
$\frac{dv}{dt} = -vg_v^{+}$
$\frac{dw}{dt} = -wg_w^{+}$
$\frac{ds}{dt} = g_{s2}(1+e^{-2k_s(u-u_s)})^{-1} - sg_{s2}$
$\frac{du}{dt} = e + wsg_{si} - g_{so}(u)$
$\frac{dv}{dt} = -vg_{v2}^{-}$
$\frac{dw}{dt} = -wg_w^{+}$
$\frac{ds}{dt} = g_{s1}(1+e^{-2k_s(u-u_s)})^{-1} - sg_{s1}$
$\frac{du}{dt} = e - ug_{o1}$
$\frac{dv}{dt} = (1-v)g_{v1}^{-}$
$\frac{dw}{dt} = (1 - ug_{w\infty} - w)g_w^{-}(u)$
$u < \theta_v$
$u \geq \theta_0$
$u \geq \theta_w$
$u < \theta_w$
$u < \theta_0$
$u \geq \theta_v$

## Example: Cardiac-Cell Model

- Using our tool dReal, we check the safety property "globally $u < \theta_v$".

  "When the property is violated, the cardiac cells lose excitability, which would trigger a spiral rotation of electrical wave and break up into a disordered collection of spirals (fibrillation)."



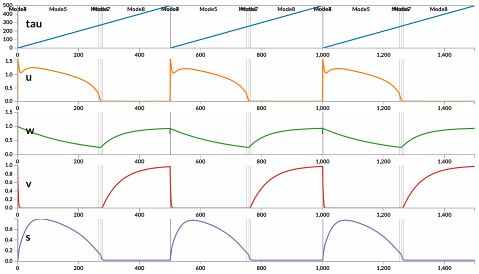
## Example: Cardiac-Cell Model

Using Bounded Model Checking with dReal as the backend engine, we successfully verified reachability properties in the cardiac-cell model.

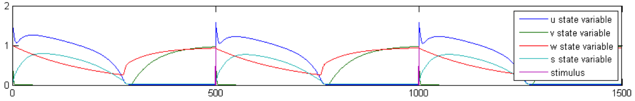
- The formulas we solved contain over 200 highly nonlinear ODEs and over 600 variables.
- Counterexamples found by dReal are confirmed by experimental data.

# dReal Result vs. Experimental Data

Counterexample computed by dReal:



Experimental data:



## Conclusion

- Turing's original goal of understanding numerical computation has become important in design and analysis of cyber-physical systems.
- We can utilize the notion of computability over the reals in formal verification of such systems.
- Practical solver: dReal (open-source at dreal.cs.cmu.edu).
- Current applications:
    - Completing formal proofs for the Kepler Conjecture
    - Finding parameters for cancer treatment models
    - Verifying safety of autonomous vehicles